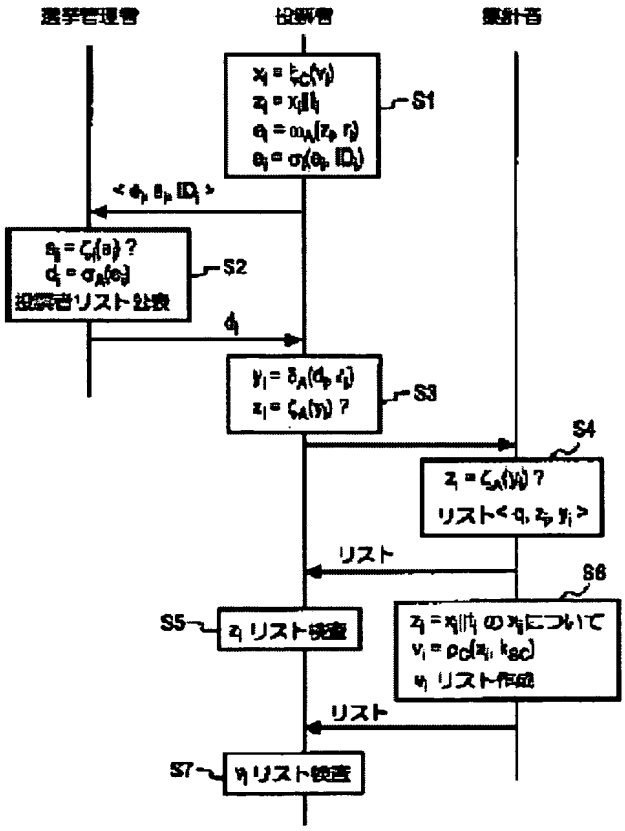
ELECTRONIC VOTING METHOD, VOTING SYSTEM AND PROGRAM RECORDING MEDIUI

Publication number: JP2000207483
Publication date: 2000-07-28
Inventor: FUJIOKA ATSUSHI; ABE MASAYUKI; MIURA FUMIMITSU
Applicant: NIPPON TELEGRAPH & TELEPHONE
Classification:
- international: ***G06F19/00; G09C1/00; H04L9/32;*** **G06F19/00; G09C1/00; H04L9/32;** (IPC1-7): G06F19/00; G09C1/00; H04L9/32
- european:
Application number: JP19990310468 19991101
Priority number(s): JP19990310468 19991101; JP19980320173 19981111

Abstract of **JP2000207483**

PROBLEM TO BE SOLVED: To unnecessitate to send a key used to encipher voting contents by a voter to a vote counting person. SOLUTION: A voter Vi enciphers voting contents vi with a public key kPC of a vote counter C, connects a tag ti to the enciphered voting contents Xi to make it zi, disturbs zi with a random number ri to prepare a pre-processing sentence ei and sends a signatures si for the pre-processing sentence and the sentence ei to an electron overseeing officer A. The officer A prepares a blind signature di for the sentence ei and returns it to the voter Vi. The voter obtains the signature information of the electron overseeing officer obtained by eliminating the effect of the number ri from the signature di and sends voting data (zi and yi) to the counter C. The counter C verifies the signature yi of the electron overseeing officer, produces a voting list including the data (zi and yi) when the signature is legitimate and opens it to the voter. The voter Vi checks the voting list to confirm that data (zi and yi) in which a tag ti included in zi coincides with the voter's tag exists in the list. The counter C decodes xi in zi to obtain the voting contents and counts the number of voting for a candidate.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－207483
（P2000－207483A）
(43)公開日　平成12年７月28日(2000.7.28)

(51)Int.Cl.[7]	識別記号	Ｆ Ｉ		テーマコード（参考）
Ｇ０６Ｆ　19/00		Ｇ０６Ｆ　15/28	Ｂ	
Ｇ０９Ｃ　1/00	６４０	Ｇ０９Ｃ　1/00	６４０Ｂ	
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７５Ｄ	

審査請求　有　　請求項の数30　ＯＬ　（全 14 頁）

(21)出願番号　特願平11－310468

(22)出願日　平成11年11月１日(1999.11.1)

(31)優先権主張番号　特願平10－320173
(32)優先日　平成10年11月11日(1998.11.11)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　藤岡　淳
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　阿部　正幸
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　三浦　史光
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(74)代理人　100066153
弁理士　草野　卓　（外１名）

(54)【発明の名称】　電子投票方法、投票システム及びプログラム記録媒体

(57)【要約】
【課題】　投票者が投票内容の暗号化に使用した鍵を集計者に送る必要をなくす。
【解決手段】　投票者V_iは投票内容v_iを集計者Ｃの公開鍵k_{pC}で暗号化し、その暗号化投票内容x_iにタグt_iを連結してz_iとし、z_iを乱数r_iで撹乱して前処理文e_iを作り、その前処理文に対する署名s_iと前処理文e_iを選挙管理者Ａへ送る。選挙管理者Ａは前処理文e_iに対するブラインド署名d_iを作成して投票者V_iへ返す。投票者はブラインド署名d_iから乱数r_iの影響を除去した選挙管理者の署名情報y_iを得、投票データ$<z_i, y_i>$を集計者Ｃへ送る。集計者Ｃは選挙管理者の署名y_iを検証し、合格したらデータ$<z_i, y_i>$を含む投票リストを作り、投票者に公開する。投票者V_iはその投票リストを検査し、z_i中のタグt_iが自分のものと一致するデータ$<z_i, y_i>$がリストにあることを確認する。集計者Ｃはz_i中のx_iを復号化して投票内容v_iを得、候補に対する投票数を集計する。

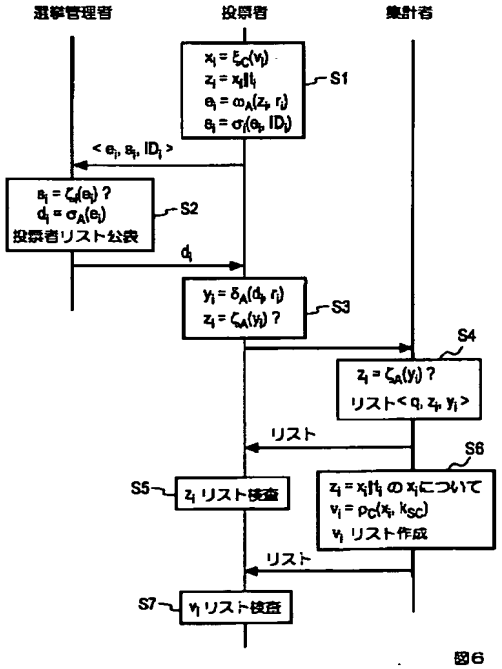


図6

1

【特許請求の範囲】

【請求項１】 管理者から投票の承認を得て投票者が集計者装置に投票データを送り、集計者装置が投票を集計する電子投票方法において、以下のステップを含む：

(a) 各投票者は、選択した候補に対応する投票内容を集計者装置の公開鍵を使って暗号化器により暗号化し、

その暗号化投票内容を含む情報を乱数により攪乱して前処理文を作成し、管理者装置に送信し、

(b) 上記管理者装置は、各投票者装置の正当性を確認し、

受信した前処理文を署名作成器に入力して前処理文に対するブラインド署名を生成し、これを投票者装置に送り返し、

(c) 各投票者は、受信した前処理文に対するブラインド署名から上記乱数成分の影響を取り除き、

上記暗号化投票内容を含む情報に対する上記管理者の管理者署名を求め、その管理者署名と上記暗号化投票内容を含む情報を集計者装置へ投票データとして送信し、

(d) 上記集計者は、上記公開鍵に対応する秘密鍵を使って復号器により上記暗号化投票内容を含む情報を復号して投票内容を得て、上記投票内容に対応する候補の得票を集計する。

【請求項２】 請求項１の電子投票方法において、上記ステップ(d) に先立って、集計者が、受信した上記暗号化投票内容と上記署名情報を署名検査器に入力して前処理文が上記管理者によって署名されていることを確認し、暗号化投票内容を含む情報をリストを公表するステップ(d-0) と、上記投票者が、自分の暗号化投票内容が表に存在することを確認するステップ(d-1) とを更に含む。

【請求項３】 請求項１又は２の電子投票方法において、上記暗号化投票内容を含む情報を攪乱するステップ(a) は、上記投票者のみが知っているタグを生成するステップと、上記暗号化投票内容と上記タグを連結して上記乱数により攪乱するステップを含み、上記ステップ(d-1) は上記表中の投票データから上記タグを分離し、そのタグが自分のものであるかを検査するステップを含む。

【請求項４】 請求項１又は２の電子投票方法において、上記ステップ(b)は上記ブラインド署名を与えた投票者を表す情報のリストを投票者リストとして公表するステップを含み、上記ステップ(c) は上記投票者リストに自分を表す情報が含まれていることを確認するステップを含む。

【請求項５】 請求項１又は２の電子投票方法において、上記ステップ(d)は上記投票内容の集計結果を公表するステップを含む。

【請求項６】 請求項１又は２の電子投票方法において、上記ステップ(a)において上記投票者は上記前処理文に投票者識別情報を付けて上記管理者装置に送信し、

2

上記ステップ(b) において上記管理者は上記投票者識別情報に基づいて上記投票者を確認し、上記ステップ(c) において上記投票者は上記投票データを無記名で上記集計装置に送信する。

【請求項７】 請求項１又は２の電子投票方法において、上記ステップ(a)は上記投票分に対する投票者の署名を生成し、上記投票分と共に上記管理者装置に送信するステップを含み、上記ステップ(b) は上記投票分に対する上記投票者の署名の正当性を検査するステップを含む。

【請求項８】 請求項１の電子投票方法において、上記集計者装置は複数のシリーズ接続された分散集計者装置を有し、それぞれの分散集計者装置は異なる集計者により管理され、上記秘密鍵は上記複数の分散集計者装置に分割してそれぞれ分散秘密鍵として割り当てられており、上記ステップ(c) で各投票者は上記投票データを上記シリーズの一端の分散集計者装置に送信し、上記ステップ(d)は上記集計者装置がそれぞれが備える復号処理部により上記分散秘密鍵を用いて上記暗号化投票内容を含む情報をシリーズに順次復号処理し、最終段の復号処理により上記投票内容を得るステップを含む。

【請求項９】 請求項１の電子投票方法において、上記集計者装置は複数の分散集計者装置を有し、それぞれの分散集計者装置は異なる集計者により管理され、上記秘密鍵は上記複数の分散集計者装置に分割してそれぞれ分散秘密鍵として割り当てられており、上記ステップ(c) で各投票者は上記投票データを全ての上記分散集計者装置に送信し、上記ステップ(d) は上記集計者装置がそれぞれが備える復号処理部により上記分散秘密鍵を用いて上記暗号化投票内容を別々に復号処理して復号中間データを生成し、予め決めた１つの分散集計者装置に集め、復号処理をして上記投票内容を得るステップを含む。

【請求項１０】 請求項８又は９の電子投票方法において、上記復号処理は、上記分散集計者装置の２以上の予め決めた数以上が動作をすれば復号可能な閾値付復号処理である。

【請求項１１】 複数の投票者装置と、各上記投票者装置と記名通信路で接続された管理者装置と、各上記投票者装置と無記名通信路で接続された電子投票システムにおいて、

各上記投票者装置は、

投票内容を集計者装置の公開鍵で暗号化して暗号化投票内容を生成する暗号化器と、

乱数を発生する乱数発生器と、

上記暗号化投票内容を上記乱数で攪乱して前処理文を作成する攪乱器と、

上記前処理文を上記管理者装置へ送信する手段と、

上記管理者装置から受信した上記管理者装置の上記前処理文に対するブラインド署名から上記乱数の影響を取り除いて上記暗号化投票内容を含む情報に対する上記管理

者装置の管理者署名を求める乱数成分除去器と、
上記管理者署名と上記暗号化投票内容を含む情報とを投票データとして集計者装置へ送信する手段とを含み、
上記管理者装置は、
受信した上記前処理文に対しブラインド署名を生成するブラインド署名作成器と、
上記ブラインド署名を投票者装置へ送信する手段とを含み、
上記集計者装置は、
上記公開鍵に対応する秘密鍵により上記投票データ中の上記暗号化投票内容を含む情報を復号して上記投票内容を得る復号器と、
上記復号された投票内容に基づいて候補に対する得票を集計する集計器とを含む。

【請求項１２】　請求項１１の電子投票システムにおいて、上記投票者装置は更に、上記暗号化投票内容を含む情報に対する上記管理者署名を検証する管理者署名検査器を含み、その管理者署名検査器による検証に合格すると上記投票データを上記集計者装置へ送信し、上記集計者装置は各上記投票者装置から受信した上記投票データ中の上記暗号化投票内容を含む情報と上記管理者署名を入力して上記管理者署名を検証する管理者署名検査器を含む。

【請求項１３】　請求項１１の電子投票システムにおいて、上記投票者装置は更に上記前処理文に対する投票者署名を生成上記管理者装置へ送信する投票者署名作成器を含み、上記管理者装置は各投票者装置から受信した上記前処理文及びその投票者署名を検証する投票者署名検査器を含み、その検証に合格すると上記ブラインド署名作成器により上記ブラインド署名を作成する。

【請求項１４】　請求項１１の電子投票システムにおいて、上記集計者装置は上記管理者署名の検証に合格すると各上記投票者装置から受信した上記投票データのリストを投票リストとして作成し、上記投票者にアクセス可能に公表する投票リスト作成器を含み、上記投票者装置は上記集計者装置から受信した投票リストに自己の暗号化投票内容が存在するか否かを検査する投票リスト検査器とを含む。

【請求項１５】　請求項１４の電子投票システムにおいて、上記投票者装置は、上記投票者のみが知っているタグを生成するタグ発生器と、上記暗号化投票内容と上記タグを連結して上記暗号化投票内容を含む情報を生成する連結器と、上記投票リスト中の各投票データから上記タグを抽出し、そのタグが自分のものであるかを検査することにより自分の投票データが上記投票リストにあるかを検査するリスト検査部を含む。

【請求項１６】　請求項１１の電子投票システムにおいて、上記集計者装置はそれぞれ異なる集計者により管理される、複数のシリーズ接続された分散集計者装置を有し、上記秘密鍵は上記複数の分散集計者装置に分割してそれぞれ分散秘密鍵として割り当てられており、各上記投票者装置は上記投票データを上記シリーズの一端の分散集計者装置に送信し、上記分散集計者装置はそれぞれ割り当てられた上記分散秘密鍵を用いて上記暗号化投票内容を含む情報をシリーズに順次復号処理する復号処理部を有し、最終段の上記分散集計者装置における上記復号処理部の復号処理により上記投票内容を得る。

【請求項１７】　請求項１１の電子投票システムにおいて、上記集計者装置はそれぞれ異なる集計者により管理される複数の分散集計者装置を有し、上記秘密鍵は上記複数の分散集計者装置に分割してそれぞれ分散秘密鍵として割り当てられており、各上記投票者装置は上記投票データを全ての上記分散集計者装置に送信し、上記上記分散集計者装置はそれぞれ割り当てられた上記分散秘密鍵を用いて上記暗号化投票内容を別々に復号処理して復号中間データを生成し、予め決めた１つの上記分散集計者装置に送る復号処理部を有しており、上記予め決めた１つの上記分散集計者装置は集められた全ての上記復号中間データを復号処理して上記投票内容を得る統合復号部を有している。

【請求項１８】　請求項１６又は１７の電子投票システムにおいて、上記復号処理部は、上記分散集計者装置の２以上の予め決めた数以上が動作をすれば復号可能な閾値付復号処理を行う。

【請求項１９】　複数の投票者装置と、各上記投票者装置と記名通信路で接続された管理者装置と、各上記投票者装置と無記名通信路で接続された集計者装置を含む電子投票システムにおける、投票者装置であって、
投票内容を集計者装置の公開鍵で暗号化し、暗号化投票内容を生成する暗号化器と、
乱数を発生する乱数発生器と、
上記暗号化投票内容を含む情報を上記乱数により攪乱して前処理文を作成する攪乱器と、
上記前処理文に対する投票者署名を生成する投票者署名作成器と、
上記前処理文及びその投票者署名を管理者装置へ送信する手段と、
上記管理者装置から受信した、上記前処理文に対する管理者のブラインド署名と上記乱数を入力して上記ブラインド署名から上記乱数の影響を取り除いて上記暗号化投票内容を含む情報に対する上記管理者の署名を求める乱数成分除去器と、
上記暗号化投票内容に対する上記管理者の署名と上記暗号化投票内容を含む情報を入力して、上記管理者の署名を検証する署名検査器と、
その署名検査器の検証に合格すると上記管理者の署名と上記暗号化投票内容を含む情報を投票データとして集計者装置へ送信する手段と、
上記集計者装置から受信した投票リストの中に自己の投票データが存在するか否かを検査するリスト検査部、と

を含む。

【請求項２０】　請求項１９の投票者装置において、更に上記投票者のみが知っているタグを生成するタグ発生器と、上記暗号化投票内容と上記タグを連結して上記暗号化投票内容を含む情報を生成する連結器とを含み、上記リスト検査部は上記集計者装置から受信した上記投票リスト中の各投票データから上記タグを抽出し、そのタグが自分のものであるかを検査することにより自分の投票データが上記投票リストの中にあるかを検査する。

【請求項２１】　複数の投票者装置と、各上記投票者装置と記名通信路で接続された管理者装置と、各上記投票者装置と無記名通信路で接続された集計者装置を含む電子投票システムにおける、集計者装置であって、

各上記投票者装置から投票データとして受信した、集計者の公開鍵で暗号化された暗号化投票内容を含む情報と上記暗号化投票内容を含む情報に対する管理者の署名とを入力して上記管理者の署名を検証する管理者署名検査器と、

上記管理者署名の検証に合格すると各上記投票者装置から受信した上記投票データのリストを作成し、上記投票者にアクセス可能に公表する投票リスト作成器と、

上記公開鍵に対応する秘密鍵により上記暗号化内容を含む情報を復号して投票者の投票内容を得る復号器と、

上記復号された投票内容に基づいて候補に対する得票を集計する集計器、とを含む。

【請求項２２】　請求項２１の集計者装置はそれぞれ異なる集計者により管理される、複数のシリーズ接続された分散集計者装置を有し、上記秘密鍵は上記複数の分散集計者装置に分割してそれぞれ分散秘密鍵として割り当てられており、各上記投票者装置から送られた上記投票データは上記シリーズの一端の分散集計者装置により受信され、上記分散集計者装置は、それぞれ割り当てられた上記分散秘密鍵を用いて上記暗号化投票内容を含む情報をシリーズに順次復号処理する分散復号処理部を有し、最終段の上記分散集計者装置における上記分散復号処理部の復号処理により上記投票内容を得る。

【請求項２３】　請求項２１の集計者装置はそれぞれ異なる集計者により管理される複数の分散集計者装置を有し、上記秘密鍵は上記複数の分散集計者装置に分割してそれぞれ分散秘密鍵として割り当てられており、各分散集計者装置は全ての上記投票者装置から上記投票データを受信し、割り当てられた上記分散秘密鍵を用いて上記暗号化投票内容を復号処理して復号中間データを生成し、予め決めた１つの上記分散集計者装置に送る分散復号処理部を有しており、上記予め決めた１つの上記分散集計者装置は集められた全ての上記復号中間データを復号処理して上記投票内容を得る統合復号部を有している。

【請求項２４】　請求項２２又は２３の集計者装置において、上記分散復号処理部は、上記分散集計者装置の２以上の予め決めた数以上が動作をすれば復号可能な閾値付復号処理を行う。

【請求項２５】　複数の投票者装置と、各上記投票者装置と記名通信路で接続された管理者装置と、各上記投票者装置と無記名通信路で接続された集計者装置を含む電子投票システムにおける投票者装置の処理手順をコンピュータで実行するプログラムを記録した記録媒体であって、上記処理手順は以下のステップを含む：

(a) 投票内容を集計者装置の公開鍵で暗号化して暗号化投票内容を生成し、

(b) 乱数を発生し、

(c) 上記暗号化投票内容を含む情報を上記乱数で攪乱して前処理文を作成し、

(d) 上記前処理文の署名を生成し、

(e) 上記前処理文及びその署名を選挙管理者装置へ送信し、

(f) 上記乱数を用いて、選挙管理者装置から受信した上記前処理文に対する上記管理者のブラインド署名から上記乱数の影響を取り除いて上記暗号化投票内容を含む情報に対する上記管理者の署名を求め、

(g) 上記暗号化投票内容を含む情報の正当性を検証し、

(h) 上記正当性の検証に合格すると上記暗号化投票内容を含む情報と上記管理者の署名を投票データとして集計者装置へ送信し、

(i) 上記集計者装置から受信した投票リストに自己の投票データが存在するか否かを検査する。

【請求項２６】　請求項２５の記録媒体において、処理手順は更に上記投票者のみが知っているタグを生成するステップと、上記暗号化投票内容と上記タグを連結して上記暗号化投票内容を含む情報を生成するステップとを含み、上記ステップ(i) は上記集計者装置から受信した上記投票リスト中の各投票データから上記タグを抽出し、そのタグが自分のものであるかを検査することにより自分の投票データが上記投票リストの中にあるかを検査するステップを含む。

【請求項２７】　複数の投票者装置と、各上記投票者装置と記名通信路で接続された管理者装置と、各上記投票者装置と無記名通信路で接続された集計者装置を含む電子投票システムにおける集計者装置の処理手順をコンピュータで実行するプログラムを記録した記録媒体であって、上記処理手順は以下のステップを含む：

(a) 各上記投票者装置から投票データとして受信した、集計者の公開鍵で暗号化された暗号化投票内容を含む情報と上記暗号化投票内容を含む情報に対する管理者の署名とを入力して上記管理者の署名を検証し、

(b) 上記管理者署名の検証に合格すると各上記投票者装置から受信した上記投票データのリストを投票リストとして作成し、その投票リストを投票者がアクセス可能に公開し、

(c) 上記公開鍵に対応する秘密鍵により上記暗号化内容

を含む情報を復号して投票者の投票内容を得、
(d) 上記復号された投票内容に基づいて候補に対する得票を集計する。

【請求項２８】 請求項２７の記録媒体において、上記集計者装置はそれぞれ異なる集計者により管理される、複数のシリーズ接続された分散集計者装置を有し、上記秘密鍵は上記複数の分散集計者装置に分割してそれぞれ分散秘密鍵として割り当てられており、上記ステップ(c) は各上記投票者装置から送られた上記投票データを上記シリーズの一端の分散集計者装置により受信し、それぞれの上記分散集計者装置により、割り当てられた上記分散秘密鍵を用いて上記暗号化投票内容を含む情報をシリーズに順次分散復号処理するステップを有し、最終段の上記分散集計者装置における上記分散復号処理により上記投票内容を得る。

【請求項２９】 請求項２７の記録媒体において、上記集計者装置はそれぞれ異なる集計者により管理される複数の分散集計者装置を有し、上記秘密鍵は上記複数の分散集計者装置に分割してそれぞれ分散秘密鍵として割り当てられており、上記ステップ(c) は各分散集計者装置により全ての上記投票者装置から上記投票データを受信し、割り当てられた上記分散秘密鍵を用いて上記暗号化投票内容を復号処理して復号中間データを生成し、それを予め決めた１つの上記分散集計者装置に送り、上記予め決めた１つの上記分散集計者装置は集められた全ての上記復号中間データを統合復号処理して上記投票内容を得るステップを有している。

【請求項３０】 請求項２８又は２９の記録媒体において、上記ステップ(c) は上記分散集計者装置の、２以上の予め決めた数以上が動作をすれば復号可能な閾値付分散復号処理を行う。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、電気通信システムでアンケート調査等を行う場合に、安全な無記名投票を実現しようとする電子投票システム、投票方法及びプログラム記録媒体に関する。

【０００２】

【従来の技術】投票とは、有権者全員に提示された複数の候補から各投票者が予め指定された数（１又は２以上）の候補を選択し、その選択結果を集計者に与え、集計者は各候補に対する投票数を集計することである。候補としては、政治的選挙における立候補者の名前のみならず、統計調査における選択項目であってもよい。また、投票内容は、投票者が選択した候補を表す識別情報、記号、名前、項目などである。

【０００３】無記名投票は、投票者と投票内容の対応を秘密にでき、個人の思想信条に関するプライバシーを守るのに適しているので、電子会議やＣＡＴＶ等の双方向通信でのアンケート調査等に利用できる。

【０００４】電気通信において、安全な無記名投票を行うには、投票者の偽装や二重投票、投票内容の盗聴に伴う投票内容の漏洩等の防止が必要である。これらの問題を解決する方法として、ディジタル署名を用いた電子投票方式が提案されており、例えば、Atsushi Fujioka, Tatsuaki Okamoto, Kazuo Ohta: “A practical secretvoting scheme for large scale elections”, in Advances in Cryptology-AUSCRYPT'92, Lecture Notes in Computer Science 718, Springer-Verlag, Berlin, pp.244-251(1993)、日本国特許出願公開6-19943（1994年11月28日公開）「電子投票方法及び装置」に示されている。

【０００５】この従来法では、投票者V_iが投票内容v_iを鍵k_iにより暗号化して暗号文x_iとし、これにブラインド署名を得るための前処理としてxiを乱数r_iにより攪乱して前処理文e_iを作成し、前処理文e_iに投票者の署名s_iを付けて選挙管理者Ａに送信する。選挙管理者Ａは署名s_iに基づいて投票者V_iの正当性を認証した後、前処理文e_iに選挙管理者のブラインド署名d_iを付けて投票者に返送する。投票者V_iは前処理文e_iに対するブラインド署名d_iから暗号文x_iに対する選挙管理者Ａの署名y_iを求め、これを暗号文x_iと共に集計者Ｃに送信する。集計者Ｃは暗号文x_iが選挙管理者Ａにより署名されていることを確認して、暗号文x_iをそのまま一覧公開する。投票者V_iは自分の暗号文x_iが登録されている場合は、投票内容v_iの暗号化に使用した鍵k_iを集計者Ｃに送り、登録されてない場合は集計者Ｃに対して異議を申し立てる。集計者Ｃは投票者から受信した鍵k_iを使って暗号文x_iから投票内容v_iを復号し、これを集計する。

【０００６】

【発明が解決しようとする課題】しかしながら、この方法では、投票者V_iが投票締切後に公開された投票一覧から自分の暗号文x_iが登録されたことを確認し、鍵k_iを集計者Ｃに送信することが必要であり、即ち、投票者の利便性の低いシステムである。

【０００７】この発明の目的は、プライバシーを侵すことなく異議申し立てが行え、また、集計者の不正や機能不全に対処できると共に、投票後に投票者が暗号化に使用した鍵を集計者に送る必要のない、簡便な電子投票システム及びその方法を提供することにある。

【０００８】

【課題を解決するための手段】この発明では、投票者が投票内容を集計者の公開鍵で暗号化し、更にその暗号化投票内容を乱数で攪乱して前処理文を作成して、その前処理文に署名を付けて選挙管理者に送信する。選挙管理者は、付加された署名を用いて投票者の正当性を認証した後に、前処理文にブラインド署名して前処理文に対するブラインド署名を各投票者に送り返す。投票者は前処理文に対するブラインド署名から乱数の影響を取り除いて暗号化投票内容に対する選挙管理者の署名情報を求め、暗号化投票内容と共に投票データとして集計者に送

信する。集計者は受信した暗号化投票内容に対する署名情報が選挙管理者によって署名されていることを確認した後に、投票データを公開する。それぞれの投票者が、公開された投票データのリストに自分の暗号化投票内容が登録されていることを確認した後に、集計者は、自らが保持する秘密鍵を用いて暗号化投票内容から投票内容を取り出し、これを集計する。もし、投票リストに暗号化投票内容が登録されていない場合には、集計者に対して異議を申し立てる。また、集計者を複数とし、それぞれが復号化鍵の一部を保持し、集計者全員もしくは一定数が協力することによって、暗号化投票内容からすべての投票内容を取り出すようにしてもよい。

【０００９】この発明によれば、暗号化投票内容は投票内容を乱数で攪乱しているので、選挙管理者、及び集計者は、攪乱された投票内容から投票内容を求めることが出来ず、投票の無記名性が保障できる。

【００１０】ここで、復号化鍵は集計者が保持しており、投票者は、開票のために再度集計者へ通信を行なう必要がない。

【００１１】集計者を複数とすれば、それらが協力することにより暗号化された投票内容を開票する場合は、異議申し立て時に、自分が正当な投票者であることは、暗号化されている投票内容と選挙管理者の署名を送るだけで示すことができる。即ち、複数存在する集計者の一部に不正者が存在したとしても、全員もしくは一定数の集計者が協力しないかぎり投票内容が明らかになることはない。

【００１２】また、分散された集計者には、暗号化された投票内容が集まるので、この場合も全員もしくは一定数の集計者が協力しないかぎり、投票の間にその途中経過は明らかにならないので、公平な投票方式となっている。

【００１３】更に、集計者全員でなく一定数が協力するだけで開票が可能な場合は、集計者内の何人かが不正者、もしくは、開票への協力が不可能となっても、正しく開票作業を行なうことができるので、この方式は耐故障性の高いシステムであると言える。

【００１４】

【発明の実施の形態】以下の実施例の説明においては、投票の例として政治的選挙における投票にこの発明を適用した場合について説明するが、前述したように、この発明の意図する投票原理は統計調査における投票にもそのまま適用できる。

第１実施例

図１はこの発明による投票システムの全体構成を示す図である。Ｔ人の投票者V_i（i=1,…,T）の装置（投票者装置と呼ぶ）100 は、選挙管理者Ａの装置（選挙管理者装置と呼ぶ）200 と、また集計者Ｃの装置（集計者装置と呼ぶ）300 と、それぞれ記名通信路400 、及び無記名通信路500 を介して接続されている。投票者V_iが記名通信路400 を通して選挙管理者Ａに情報を送信する場合には、その情報に送信者が誰であるかを示す送信者情報、例えば氏名V_i又は識別情報ID_iを付加して送信するものとし、無記名通信路500 を通して集計者Ｃに情報を送信する場合には、その情報に送信者情報を付加しないものとする。また、集計者Ｃは投票内容の一覧（投票リスト及び得票数リスト）を公開し、投票者は全員、これにアクセスが可能であるとする。図３に図１の投票システムにおける投票者装置100 の構成例を、図４に選挙管理者装置200 の構成例を、図５に集計者装置300 の構成例を示し、図６にこの発明の投票システムにおける通信シーケンス例を示す。また、図２Ａに選挙管理者Ａが有している有権者リスト240Aを、図２Ｂに投票承認を与えた投票者リスト240Bを、図２Ｃに集計者Ｃが作成した投票後で、かつ集計前の投票リスト320Aを、図２Ｄに集計後の投票リスト320Aを、図２Ｅに得票数リスト320Bを例示する。

【００１５】以下では、特に投票者V_iが選挙管理者Ａから投票の承認を得た後に、集計者Ｃに対して投票手続きする場合について説明する。

【００１６】ここで、以下の説明に使用される記法をまとめて示す。

【００１７】$x=\xi_c(v,k_{pc})$：集計者Ｃの暗号化関数（ｘ：暗号文、ｖ：投票内容、k_{pc}：集計者の公開鍵）

$v=\rho_c(x,k_{sc})$：集計者Ｃの復号化関数（k_{sc}：集計者の秘密鍵）

$s=\sigma_i(e)$：投票者V_iの署名作成関数（ｓ：署名、ｅ：暗号化投票内容）

$e=\xi_i(s)$：投票者V_iの署名に対する検証関数

$d=\sigma_A(e)$：選挙管理者Ａのブラインド署名作成関数（ｄ：ブラインド署名）

$z=\xi_A(y)$：選挙管理者Ａの署名に対する検証関数（ｙ：署名、ｚ：投票用紙）

$e=\omega_A(z,r)$：攪乱関数（ｒ：乱数）

$y=\delta_A(d,r)$：乱数成分除去関数（ｄ：ブラインド署名）

ここで、集計者Ｃの暗号化関数ξ_cと復号化関数ρ_cは周知の公開鍵暗号方式で使用されているものであり、集計者Ｃは秘密鍵k_{sc}を秘密に保持し、公開鍵k_{pc}を投票者に公開しているものとする。また、投票者がブラインド署名を要求する際に署名対象のメッセージｍを乱数ｒでブラインドする（ブラインド署名のための前処理をする）ための攪乱関数$\omega_A(z,r)$と、受け取ったブラインド署名ｄから乱数成分ｒを除去して投票用紙ｚに対する選挙管理者Ａの署名ｙを取り出す。乱数成分除去関数$\delta_A(d,r)$は、選挙管理者Ａが使用するブラインド署名関数σ_Aが決まれば、必然的に決まるものである。このような署名関数については、例えばＲＳＡ暗号の暗号化関数と復号化関数があり（Ronald Rivest, Adi Shamir, Leonard Adleman：“A method for obtaining digital sig

natures and public-keycryptosystems", Communications of the ACM, Vol.21, No.2, pp.120-126(Feb., 1978)), ブラインド署名を要求するための前処理としての乱数による攪乱の手法についての詳細は、David Chaum : "Security without identification : Transaction systems to make big brother obsolete", Communications ofthe ACM, Vol.28, No.10, pp.1030-1044(Oct., 1985)に記述されている。

【００１８】図３に示す投票者装置100 は次のように構成されている。記憶部121 には予め投票者の識別情報ID$_i$ と名前V$_i$が保持されている。また、装置100 内で生成されるデータのうち、後の処理に使用されるデータも記憶部121 に保持される。暗号化器110 は投票者V$_i$が選択した投票内容v$_i$を（ここでは例えば候補者名CND$_h$）集計者Ｃの公開鍵k$_{pc}$で暗号化し、暗号文$x_i = \xi_c(v_i, k_{pc})$を得る。タグ発生器111は乱数t$_i$を発生し、その乱数t$_i$は投票者V$_i$のみが知っているタグとして後述のように使用される。連結器112 は暗号文x$_i$とタグt$_i$を連結して$z_i = x_i \| t_i$を出力する。以降、z$_i$を投票用紙と呼ぶことにする。乱数発生器120 は乱数r$_i$を発生する。攪乱器130 はブラインド署名のための前処理として、攪乱関数$e_i = \omega_A(z_i, r_i)$により投票用紙z$_i$を乱数r$_i$で攪乱し前処理文e$_i$を生成する。署名作成器140 は前処理文e$_i$に対し投票者V$_i$のものであることを示すための署名$s_i = \sigma_i(e_i, ID_i)$を生成する。データ<e$_i$, s$_i$, ID$_i$> は送受信部190 から通信路400 を介して選挙管理者装置200 に送信される。通信路400 による選挙管理者装置200 との接続は、選挙管理者装置200 からブラインド署名d$_i$が受信されるまで維持される。

【００１９】乱数成分除去器150 は選挙管理者装置200 から送受信部190 により受信したブラインド署名d$_i$から乱数r$_i$を使って乱数成分除去関数$y_i = \delta_A(d_i, r_i)$により乱数成分を除去し、y$_i$を投票用紙z$_i$に対する選挙管理者Ａの署名として得る。署名検査部160 は検証関数$z_i = \xi_A(y_i)$が成立するかを検査することによりy$_i$が正当であるか検証する。データ<z$_i$, y$_i$>は投票データとして送受信部180 から集計者装置300 に送信される。リスト検査部170 は集計者装置300 にアクセスして送受信部180 により得た投票リスト320Aを検査する。

【００２０】図４に示す選挙管理者装置200 は有権者の識別情報ID$_i$ が予め記録された有権者リスト240A（図２Ａ）と、投票の承認を与えた投票者識別情報ID$_i$ を書き込む投票者リスト240B（図２Ｂ）とを記録するための記憶部240 と、投票者から受信した識別情報ID$_i$ が有権者リストに載っているかを検査する投票者検査部210 と、受信した投票者の前処理文e$_i$に対する投票者の署名s$_i$が正しいかを検証関数$e_i = \xi_i(s_i)$が成立するかにより検査する署名検査部220 と、正当な投票者を記憶部240 の所定の領域に書き込んで投票者リストを作成する投票者リスト作成部260と、前処理文e$_i$に対するブラインド署名d$_i = \sigma_A(e_i)$を生成する署名作成器230と、投票者装置とのデータの送受信を行う送受信部250 とを有している。

【００２１】図５に示すように、集計者装置300 は投票者装置100 から受信部360 により受信した投票データ<z$_i$, y$_i$>中の投票用紙z$_i$と選挙管理者Ａの署名y$_i$に対し検証関数$\xi_A(y_i)$を使って$z_i = \xi_A(y_i)$が成立するかを検査することにより署名y$_i$を検証する署名検査部310 と、投票リスト作成部370 により投票データ<z$_i$, y$_i$>に通し番号q$_i$を付けて投票リスト320A（図２Ｃ）に加え、保持する記憶部320 と、投票用紙$z_i = x_i \| t_i$から暗号文x$_i$を分離する分離部350 と、集計者の秘密鍵k$_{sc}$ を使って復号関数ρ_c によりx$_i$を復号して$v_i = \rho_c(x_i, k_{sc})$を投票内容として得る復号化器330 と、投票内容v$_i$を集計する集計器340 とを有する。また、記憶部320 に保持されている投票リスト320Aの通し番号q に対応する投票データに図２Ｄに示すように復号された投票内容v$_i$を追加する。集計結果は図２Ｅに示すように各候補（CND$_h$; h=1, 2, ...）の得票数C#$_h$ (h=1,2,...) を得票リスト320Bとして記憶部320 に保持される。投票リスト320Aと得票リスト320Bの内容は送受信部380 を通してアクセスした投票者装置100 に送信される。

【００２２】以下、この第一の実施例における投票の手順を図６を参照して説明する。

ステップＳ１： 投票者V$_i$は、投票者装置100 （図３）により投票の準備を以下のように行う。

【００２３】ステップS1-1： 投票者V$_i$は、投票内容v$_i$を暗号化器110 で集計者Ｃの公開鍵k$_{pc}$ と暗号化関数ξ_c により暗号化し、暗号文

$x_i = \xi_c(v_i, k_{pc})$

を作成する。更に、タグ発生器111 によりタグt$_i$を生成し、連結器112 によりx$_i$と連結して投票用紙

$z_i = x_i \| t_i$

を得る。タグt$_i$は例えば乱数であり、投票者V$_i$のみが自分のものであることを知っている。

【００２４】ステップS1-2： 投票者V$_i$は、乱数生成器120 を用いて乱数r$_i$を生成し、攪乱器130 を用いてz$_i$をr$_i$により攪乱して前処理文

$e_i = \omega_A(z_i, r_i)$

を作成する。

【００２５】ステップS1-3： 投票者V$_i$は、署名作成器140 を用いて、前処理文e$_i$と識別情報ID$_i$ に対する署名

$s_i = \sigma_i(e_i, ID_i)$

を作成し、データ<e$_i$, s$_i$, ID$_i$> を送受信部190 から選挙管理装置200 に送信する。

ステップＳ２： 選挙管理者装置200 （図４）は、登録された有権者名V$_i$とその識別情報ID$_i$ の関係を図２Ａに示すように有権者リスト240A（図２Ａ）として予め有しており、更に、投票の承認を与えた有権者の名前V$_i$又は識別情報ID$_i$ を投票者リスト作成部260 により書き込むための投票者リスト240B（図２Ｂ）を有している。投票

者リストは投票受付終了後に公開されるので、承認された投票者の名前V_iを公開してよいのであれば投票者名V_iを書き込むが、投票者の名前が知られるのを避けるのであれば識別情報ID_iを記録する。投票システムとしていずれか一方に決めておく。以下の説明では投票者V_iの識別情報ID_iを投票者リスト240B（図２Ｂ）に書き込むこととする。投票受付開始時点では、投票者リストの中には何も記録されていない。選挙管理者装置200により承認手続きを以下のように行う。

【００２６】ステップS2-1：　選挙管理者Ａは、投票者が有権者であることを、有権者リスト240A（図２Ａ）に識別情報ID_iがあるか否かを投票権確認部210により調べて確認する。もし無ければ、選挙管理者Ａは承認を拒否する。

【００２７】ステップS2-2：　選挙管理者Ａは、これ以前に投票者V_iが選挙管理者Ａによる承認を受けているか否かを、投票者リスト240B（図２Ｂ）にID_iが既に書き込まれているかを投票権確認部210により調べて検査する。もし、ID_iが既に承認されていたならば、選挙管理者Ａは二重投票として承認を拒否する。

【００２８】ステップS2-3：　ID_iがまだ書き込まれて無ければ、選挙管理者Ａは、署名検査器220を用いて、s_iとe_i，ID_iが次式

$$(e_i, ID_i) = \xi_A(s_i)$$

を満足するか検査する。もし、合格ならば、選挙管理者Ａは、e_iを署名作成器230に通して、署名d_i

$$d_i = \sigma_A(e_i)$$

を計算し、d_iを送受信部250から投票者装置100に送信すると共に、投票者リスト作成部260により記憶部240内の投票者リスト240B（図２Ｂ）に投票者V_iのID_iを追加する。

【００２９】ステップS2-4：　投票受付終了後、選挙管理者Ａは、投票者リスト240Bと投票者数を公表する。公表の方法は、予め有権者に所定の日時から一定期間内に任意の通信路を介して選挙管理者装置200の記憶部240内の投票者リスト240Bにアクセス可能であることを告知しておく。このリストへのアクセス方法は、例えば予め決めた電話番号により行うようにすることができる。投票者リスト240Bの公表場所は選挙管理者装置200内でなく、インターネット上の予め決めたアドレスに公表してもよい。

ステップＳ３：　投票者V_iは、投票者装置100（図３）により投票用紙とその署名情報を以下のように作成する。

【００３０】ステップS3-1：　投票者V_iは、d_iとr_iを乱数成分除去器150に入力して、投票用紙z_iに対する署名情報y_i

$$y_i = \delta_A(d_i, r_i)$$

を求める。

【００３１】ステップS3-2：　投票者V_iは、署名検査器160を用いて、y_iが選挙管理者Ａの署名であることを

$$z_i = \xi_A(y_i)$$

が成立するかにより確認する。もし、不合格であったなら、投票者V_iはデータ$<e_i, d_i>$を示すことにより、選挙管理者Ａの不正を主張する。

【００３２】ステップS3-3：　投票者V_iは、前記署名確認が合格であれば送受信部180からデータ$<z_i, y_i>$を集計者装置300に通信路500を通して送信する。

ステップＳ４：　集計者Ｃは、集計者装置300により以下のようにして票を収集する。

【００３３】ステップS4-1：　集計者Ｃは、投票者から受信部360により投票データ$<z_i, y_i>$を受信し、署名検査器310を用いてy_iが投票用紙z_iに対する正当な署名であることを

$$z_i = \xi_A(y_i)$$

が成立するかを検査することにより確認する。もし、合格ならば、投票リスト作成部370により投票リスト230A（図２Ｃ）に、それぞれの投票用紙z_iとその署名y_iに一連の番号qにより番号付けをし、投票データ$<q, z_i, y_i>$として掲載する。

【００３４】ステップS4-2：　すべての投票後、集計者Ｃは送受信部380を通して記憶部320にアクセス可能とすることにより投票リスト320Aを公表する。この投票リストはすべての投票者からアクセスが可能であるとする。公表方法は前述の投票者リスト２４０Ｂの場合と同様に、公表期間、公表場所、を予め告知しておく。

ステップＳ５：　投票者V_iは、投票者装置100により以下のようにして検証を行う。

【００３５】ステップS5-1：　投票者V_iは、送受信部180により集計者装置300の記憶部320をアクセスし、投票リスト320Aの内容を受信し、投票リスト320Aに掲載された投票の数がStep 2-4で公表された投票者の数と一致するかを表検査器170で検査する。もし、不合格ならば、番号qと乱数r_iを公表して、選挙管理者Ａの不正を主張する。

【００３６】ステップS5-2：　投票者V_iは、自らの投票用紙z_iが、投票リスト320Aに掲載されているかを表検査器170で検査する。その検査として、z_iそのものがリスト中にあるかを検査してもよいし、$z_i = x_i \| t_i$中のタグt_iが自分のものであるか検査してもよい。もし、掲載されていなければ、投票データ$<z_i, y_i>$を示して、集計者Ｃの不正を主張する。

ステップＳ６：　集計者Ｃは、集計者装置300により以下のようにして開票、及び、集計を行う。

【００３７】ステップS6-1：　受信部360により投票者V_iからの投票用紙z_iと署名y_iの受信開始後、前記不正の通知が所定時間内になければ、集計者Ｃは、分離部350で投票用紙$z_i = x_i \| t_i$からx_iを分離し、復号化器330にて開票し、秘密鍵k_{sc}を使って投票内容v_iを

$$v_i = \rho_c(x_i, k_{sc})$$

により求め、投票内容v_iが正しい投票か、つまり投票内容v_iが予め提示した候補を表す名前又は記号となっているかを検査する。なっていなければ無効投票とされる。

【００３８】ステップS6-2： 集計者Cは、図２Cの投票リストの投票内容v_iを集計器340を用いて集計し、各候補に対する投票数を得て、その結果を図２Eに示す得票数リスト320Bとして公表するとともに、q番目の投票データ$<x_i, t_i, y_i>$に対し図２Dに示すように、v_iを追加する。集計結果は投票リスト320Aに添付して公表する。

ステップＳ７： 投票者V_iは、投票者装置100により集計者Cの操作が正しいことを確認する。つまり図２Cに示す投票リスト320A中にすべてのv_iが追加されたか、また投票者V_iのx_iとv_iとが対応しているかを確認する。

【００３９】なお、上記ステップＳ５は省略してもよい。更に、ステップS6-2における得票数リストの公表、及びステップＳ７も省略してよい。

【００４０】前述の実施例では投票者V_iが集計者Cの暗号化関数ξ_cを使って投票内容v_iを$x_i = \xi_c(v_i, k_{pc})$と暗号化し、集計者Cに投票データ$<z_i, y_i>$を送るので、集計者Cは、もしそのつもりになればStep 4-2で投票リストを公開する前であっても集計者の秘密鍵k_{pc}を使ってz_i中のx_iを復号関数$v_i = \rho_c(x_i, k_{sc})$により復号して$v_i$を得ることができる。即ち、投票リストの公開を待たずに投票の傾向、途中結果などの情報を得て、その情報を公式の集計結果が出る前に特定な人に漏らすことができるので、選挙の公平性の点から好ましくない。また、第１実施例では、集計者装置300が故障した場合、投票の集計をスケジュール通りに完了できないこともある。以下では複数の集計者によりそれぞれ管理される複数の集計者装置により暗号化投票内容を復号し、集計することによりこれらの点について改善した実施例を説明する。

【００４１】ここで、分散集計者の暗号関数(暗号化関数ξ_c，復号化関数ρ_c)は、公開鍵暗号方式で使用されるものであるが，各暗号文x_iに対し全ての分散集計者がそれぞれもっている分散秘密鍵k_{sc1}で復号処理を行なうことではじめて、暗号文が復号可能となったり、又は復号処理に必要な人数にしきい値U_t ($2<U_t<U$)が存在し、一定数のしきい値付分散集計者が集まれば復号可能なようなものとする。このような暗号関数については、例えばElGamal 暗号（Taher ElGamal ： “A public keycrypto system and a signature scheme based on discrete logarithms ”，IEEE Transactions on Informatoin Theory, Vol.IT-31, No.4, pp.469-472(July,1985)）の暗号化関数と復号化関数があり、これの分散した復号者による復号の手法やしきい値を導入した手法についての詳細は、Yvo Desmedt, Yale Frankel： “Threshold cryptos ystems ” in Advances in Cryptology-CRYPTO'89, Lecture Notes in Computer Science 435, Springer-Verlag, Berlin, pp.307-315(1990) に記述されている。

第２実施例

図７は第２実施例による投票システムの全体の構成を示す。この実施例では、それぞれの投票者装置100 が通信路400 を介して選挙管理人装置200 に接続され，また通信路500 を通して１つの集計者装置に接続される点は第１実施例と同じであるが、構成上の異なる点は、複数の集計者装置300_j（$j=1,\cdots,U$，以下分散集計者装置と呼ぶ）を設け、分散集計者装置300_1は全ての投票者からの暗号文x_iを復号処理してx_{i1}を生成し，次の分散集計者装置300_2に送り，同様にｊ番目の分散集計者装置300_jは直前の分散集計者装置300_{j-1}から受けた復号処理データx_{ij-1}を復号処理してx_{ij}を生成し，次の分散集計者装置300_{j+1}に送る。最後の分散集計者装置300_0による復号処理により初めて投票内容v_iが得られる。第１実施例と同様に、通信路400 を通して投票者装置100_iがデータを管理者装置200 に送る場合は、投票者V_iの識別情報ID_iを付けて送るが、通信路500 を通してデータを分散集計者装置300_1に送る場合は、識別情報ID_i を付けない。

【００４２】通信シーケンス例や各投票者装置100_iの構成例、選挙管理者装置200 の構成例などは集計者装置300 を分散集計者装置300 とする以外は先と同様である。また，各投票者は共通の公開鍵k_{pc} を使って投票内容v_iを$x_i = C(v_i, k_{pc})$により暗号化する点も第１実施例と同じであるが，集計者C_1～C_Uは秘密鍵k_{sc} から生成されたU個の分散秘密鍵k_{sc1}、k_{sc2}、…、k_{scU}をそれぞれ有しており，それらを使って復号処理を行うが、各集計者装置300_j単独では暗号文x_iから投票内容v_iを復号できない。暗号システムとして前述のElGamal 暗号を使用する場合は、このような分散秘密鍵k_{sc1}，k_{sc2},…,k_{scU}を、例えばこれらの鍵の値の総和が公開鍵k_{pc}に対応する秘密鍵k_{sc} の値と等しくなるように決めることができることが前述のDesmet-Frankelの文献に示されている。

【００４３】図８Ａは投票者装置100_1～100_rからの投票を集票する第１分散集計者装置300_1の構成を示し、署名検査部310 と、記憶部320 と、集計器340 と、分離部350 と、分散復号処理部331 と、受信部360 と、投票リスト作成部370 と、送受信部380 とを有している。図５に示した第１実施例の集計者装置300 とは次の点で異なっている。第１に、分散復号処理部331 において暗号文x_iに対し分散秘密鍵k_{sc1}を使って復号処理$x_{i1} = \rho_{c1}(x_i, k_{sc1})$により復号中間データ$x_{i1}$ を生成し、それを次の分散集計者装置300_2に送ることである。第２に、集計器は最後の分散集計者装置300_0から復号投票内容v_iを受信し、それを集計することである。第２～第Ｕ分散集計者装置300_2～300_0のそれぞれは第ｊ分散集計者装置（$2 \leq j \leq U$）を代表して図８Ｂに示すように、分散復号処理部331 を有するだけであり、前段の分散集計者装置300_{j-1}から受信した復号中間データx_{ij-1}に対し、分散秘密鍵k_{sc1}を使って復号処理$x_{ij} = \rho_{c1}(x_{ij-1}, k_{sc1})$により復号中間データ$x_{ij}$ を生成し、それを次段の分散集計者装

置300_{j+1}に送信する。ただし、最終段の分散集計者装置300_Uでは復号処理$x_{iU}=\rho_{cU}(x_{iU-1}, k_{scU})$により$x_{iU}$を最終的復号結果である投票内容$v_i=x_{iU}$として得ることができ、その投票内容$v_i$を第１分散集計者装置$300_1$に送信する。

【００４４】この第２実施例における投票の手順を示す。この実施例においても、第１実施例におけるステップＳ１からステップＳ５までの手順と同じ手順が実行される。ただし、各投票者装置100_iから投票データ$<z_i, y_i>$を受けるのは第１分散集計者装置300_1であるものとする。この第２実施例は第１実施例のステップＳ６，Ｓ７を以下のように変更したものであり、Ｕは分散集計者装置の数である。

ステップＳ６：　分散集計者C_j（$j=1,\cdots,U$）は、分散集計者装置300_jにより、以下のようにして集計を行う。

【００４５】ステップS6–1：　第１分散集計者装置300_1は、各投票者装置100_i（$i=1,\cdots,T$)からの投票データ$<z_i, y_i>$中の$z_i=x_i \| t_i$を分離部350で暗号文x_iとタグt_iに分離し、分散秘密鍵k_{sc1}を使って分散復号処理部330により次の復号処理

$x_{i1}=\rho_{c1}(x_i, k_{sc1})$

を行い、復号中間データx_{i1}を得て、これを次の第２分散集計者装置300_2に送る。

【００４６】以下同様に、第ｊ分散集計者装置300_jは第j–1分散集計者装置300_{j-1}からの復号中間データx_{ij-1}に対し、分散秘密鍵k_{scj}を使って分散復号処理部330により復号処理

$x_{ij}=\rho_{cj}(x_i, k_{scj-1})$

を行い、得られた復号中間データx_{ij}を次の第j+1分散集計者装置300_{j+1}に送る。

【００４７】最後の第Ｕ分散集計者装置300_Uは、第U–1分散集計者装置からの復号中間データx_{iU-1}に対し分散秘密鍵k_{scU}を使って分散復号処理部330により復号処理

$v_i=x_{iU}=\rho_{cU}(x_i, k_{scU})$

を行うことにより投票内容v_iを得る。第Ｕ分散集計者装置300_Uは得られた投票内容が無効でないか検査する。

【００４８】ステップS6–2：　第Ｕ分散集計者C_Uは、投票内容v_iを集計器340を用いて集計し、その結果を公表するとともに、投票内容v_iを投票リストに追加する。

Step 7：　投票者V_iは、投票者装置100_iにより第Ｕ分散集計者装置300_Uの操作が正しいことを確認する。

【００４９】この様に、第２実施例では復号処理を複数の分散集計者装置300_1～300_Uにより順次行い、最後の分散集計者装置300_Uにおいて投票内容v_iが得られるので、どの分散集計者も集計開始前に単独で開票してv_iを得ることはできない。

第３実施例

図９は第３実施例における投票システム全体構成を示す。この実施例では、各投票者装置100_i（$i=1,\cdots,T$)は全ての分散集計者装置300_1～300_Uに通信路500を通して接続可能とされており、生成した投票データ$<z_i, y_i>$を全ての分散集計者装置300_1～300_Uに送信する。各投票者装置100_i及び選挙管理者装置200の構成は第１及び第２実施例の場合と同じである。

【００５０】第１～第U–1分散集計者装置300_1～300_{U-1}の構成は第ｊ分散集計者装置300_jで代表して図１０Ａに示すように、各投票者装置100_iから受信した投票データ$<z_i, y_i>$のz_iに対する署名y_iの検証を行う署名検査部310と、z_iから暗号文x_iを分離する分離部350と、暗号文に対し、分散秘密鍵k_{sc1}を使って復号処理$x_{i1}=\rho_{c1}(x_i, k_{sc1})$により復号中間データ$x_{i1}$を生成する分散復号処理部331とを有し、復号中間データx_{i1}を予め決めた１つの分散集計者装置、この例では300_Uに送信する。分散集計者装置300_Uは図１０Ｂに示すように、図１０Ａの構成に更に記憶部320と、統合復号部332と、集計器340と、前分散集計者装置3001,...,300Uから集めた投票データ$<z_i, y_i>$にそれぞれ通し番号ｑを付けて投票リスト320Aに書き込む投票リスト作成部370と、投票リスト320Aと得票数リスト320Bをアクセス可能とするため投票者装置100と送受信を行う送受信部380とが追加された構成となっている。記憶部331には受信した投票データのリストを掲載する投票リスト320Aと、集計結果を表す各候補の得票リスト320Bが形成される。統合復号部332はそれぞれの分散集計者装置300_1～300_Uで生成された復号中間データx_{i1}～x_{iU}に対し復号関数ρ_cにより復号処理$v_i=\rho_c(x_{i1},\cdots,x_{iU})$を行い投票内容$v_i$を得て、集計器340に与える。集計器340は投票内容v_iの有効性を検査し、有効であれば記憶部320内に作成した得票リストの対応する候補の得票数に１を加算する。また投票リストの対応する投票データにv_iを追加する。

【００５１】この第３実施例においても、各分散集計者装置は単独で暗号文x_iから投票内容v_iを復号することはできないので、選挙の公平性が保証される。

変形実施例１

第２及び第３実施例では、全員の分散集計者C_1～C_Uが協力しなければ暗号文x_iから投票内容v_iを復号できない。しかしながら、例えば前述のDesmedt–Frankelの方法に従って分散復号処理部331を構成することにより、少なくともＬ個（$2 \leq L \leq U-1$）の分散集計者装置があれば、公開鍵k_eにより暗号化された暗号文x_iからv_iを復号可能である。この方法を第２実施例（図７、８Ａ，８Ｂ）に適用した実施例を説明する。

【００５２】例えば分散集計者装置300_2～300_Uのいずれか１つ、例えば300_jが故障しても、その直前の分散集計者装置300_{j-1}は分散集計者装置300_jを迂回して分散集計者装置300_{j+1}に復号中間データx_{ij-1}を送る。分散集計者装置300_{j+1}は復号中間データx_{ij-1}に対し分散秘密鍵k_{scj+1}を使って$x_{ij+1}=\rho_c(x_i, k_{scj+1})$により中間復号データ$x_{ij+1}$を得て、それを更に次段の分散集計者装置$300_{j+2}$に渡せばよい。この場合に使用される分散秘密鍵

の生成方法は、例えば前述のDesmedt-Frankelの文献に示されている。また、全ての分散集計者装置300_1～300_Uの構成を図８Ａに示す構成とすれば、第１分散集計者装置300_1が故障しても、それに代わって次の段の分散集計者装置300_2が投票者装置100_1～100_Iから投票データ$<z_i, y_i>$を受信し、分散集計者装置300_1の機能を代行することができる。最終段の分散集計者装置300_Uは復号処理により得られた投票内容v_iを、代行の分散集計者装置300_2に送信すればよい。この実施例によれば、U-L 以下のいずれかの分散集計者装置が故障しても、投票の集計を行うことができる。

変形実施例２

同様に、第３実施例（図９、１０Ａ，１０Ｂ）においても、分散復号処理部331 と統合復号部332 にDesmedt-Frankel の方法を適用すれば、分散集計者装置300_1～300_{U-1}のうち少なくともＬ個（$2 \leq L \leq U-1$）以上の分散集計者装置による復号中間データが得られるならばv_iを復号することができる。例えば分散集計者装置300_1～300_{U-L}が故障した場合、残りの分散集計者装置300_{U-L+1}～300_Uからの復号中間データx_{iU-L+1}～x_{iU}を分散集計者装置300_Uの統合復号部332 に与え、それらに対する復号処理$v_i = \rho_c(x_{iU-L+1}, x_{iU-L+2}, \cdots, x_{iU})$により投票内容$v_i$を復号できる。得られた投票内容$v_i$は集計器340 により有効性が検査され、有効であれば記憶部320 内の得票リストのv_iに対応する候補の得票に１を加算する。

【００５３】この変形実施例において、全ての分散集計者装置300_1～300_Uの構成を図１０Ｂに示すものと同じに構成すれば、U-L 個以内のどの分散集計者装置が故障しても、残りの１つに対し図１０Ｂの分散集計者装置と同様の動作をさせることにより投票の集計を行うことができる。

【００５４】図３～５、８Ａ，８Ｂ，１０Ａ，１０Ｂに示す各装置はその機能構成を示したものであり、これら各機能を動作を順次行わせるための制御部を備え、また全体乃至一部をコンピュータにより実行させることもできる。

【００５５】

【発明の効果】以上に説明したように、この発明では、投票内容v_iを集計者の公開暗号鍵kPCで暗号化しているので、投票者は投票内容を復号化させるために、鍵を集計者に送信する必要がない。

【００５６】集計者を複数とした場合には、集計者全員の合意が得られなければ開票作業が開始されない。

【００５７】更に、一定数の集計者が開票できる場合には、正当な集計者がある程度集まれば開票作業が開始でき、不正者もしくは故障者の影響を除去できる。

【００５８】また、集計者が投票内容を改竄（かいざん）しても、公開された投票内容の一覧表を閲覧することで、投票内容の改竄を検出できる。即ち、自らの投票が利用されていないときには、暗号化された投票用紙z_iと選挙管理者の署名y_iを公開し、不正を主張すればよい。この際、不正な集計者の数が一定であるならば異議申し立て時のプライバシーは保証されている。

【００５９】更に、複数の集計者をおいた場合に、この発明では、暗号化鍵を用いて、投票内容を暗号化して送信しているので、投票用紙の収集の際に、集計者が途中経過を漏洩して選挙に影響を及ぼすといった不正が防止できる。

【００６０】以上より、この発明では集計者の暗号化鍵を用いて、投票者の利便性を向上させ、また、集計者を複数とすることにより、途中経過を漏洩して選挙に影響を及ぼすといった不正を解決できる。

【図面の簡単な説明】

【図１】この発明の第１実施例による投票システムの全体構成を示すブロック図。

【図２】Ａは有権者リストを示す表、Ｂは投票者リストを示す表、Ｃは投票リストを示す表、Ｄは投票リストを示す表、Ｅは得票数リスト。

【図３】投票者装置100 の機能構成例を示すブロック図。

【図４】選挙管理者装置300 の機能構成例を示すブロック図。

【図５】集計者装置400 の機能構成例を示すブロック図。

【図６】投票処理手順を示す図。

【図７】第２実施例による投票システムの全体構成を示すブロック図。

【図８】Ａは図７における分散集計者装置300_1の機能構成例を示すブロック図、Ｂは図７における分散集計者装置300_2～300_Uの機能構成を示すブロック図。

【図９】第３実施例による投票システムの全体構成を示すブロック図。

【図１０】Ａは図９における分散集計者装置300_1～300_{U-1}の機能構成を示すブロック図、Ｂは図９における分散集計者装置300_Uの機能構成を示すブロック図。

【図１】

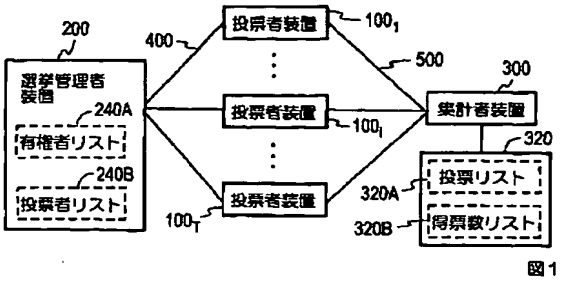


図1

【図２】

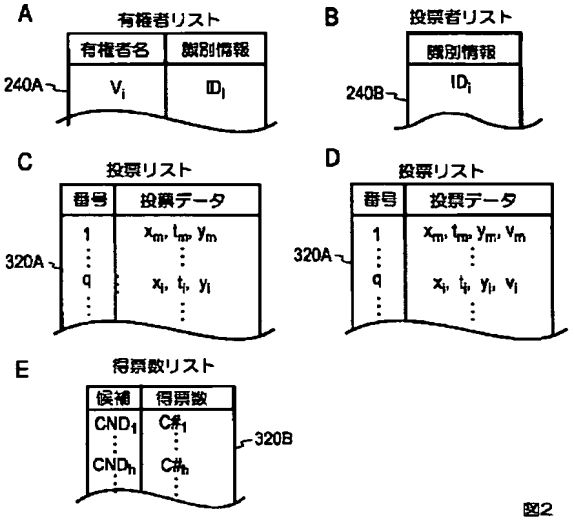


図2

【図３】

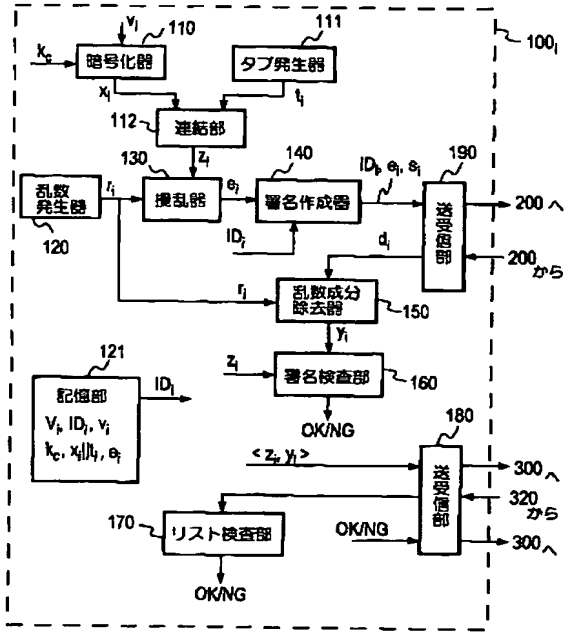


図3

【図４】

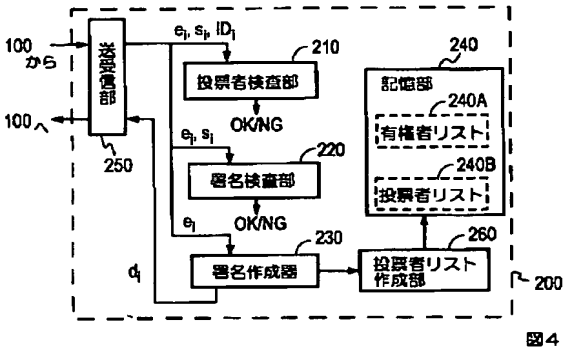


図4

【図５】

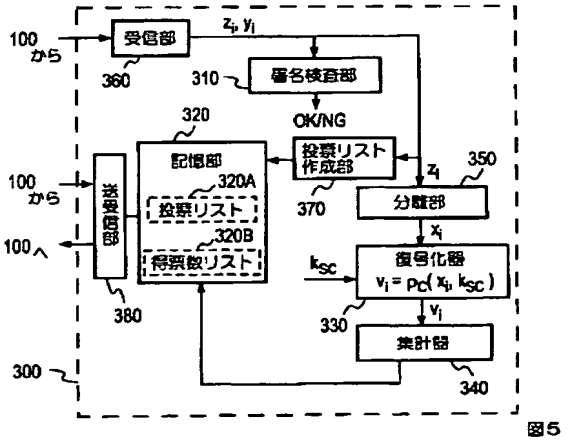


図5

【図６】

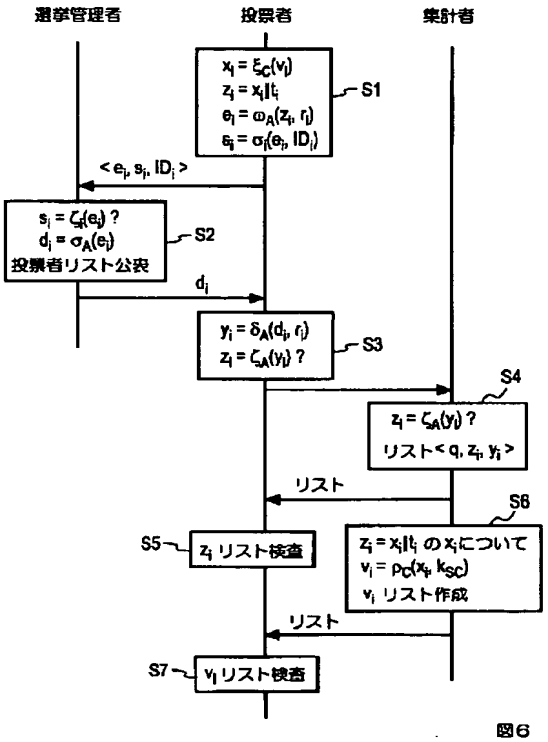


図６

【図７】

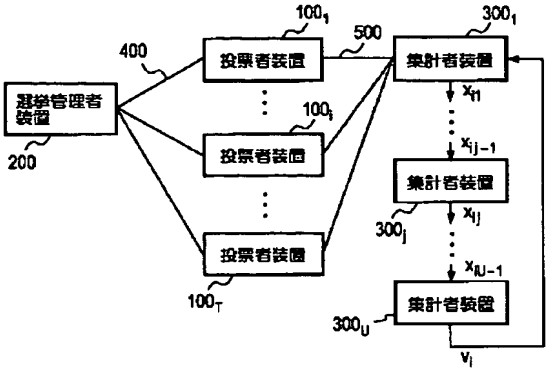


図７

【図８】

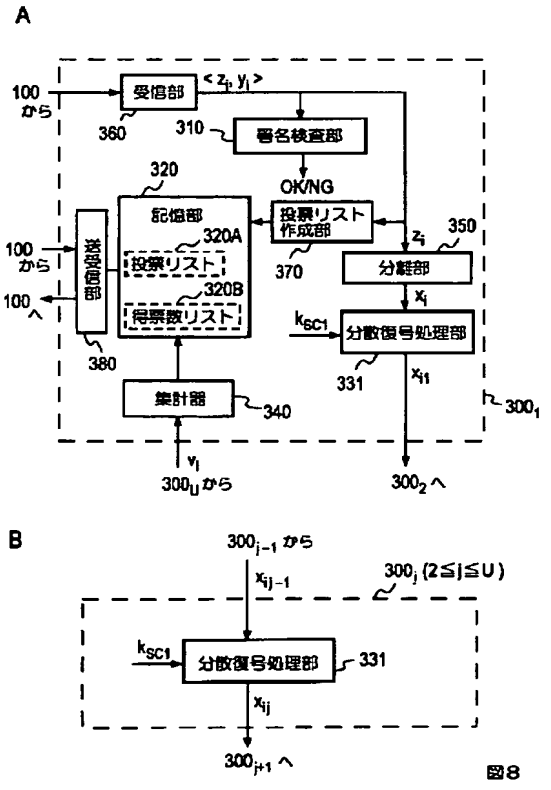


図８

【図９】

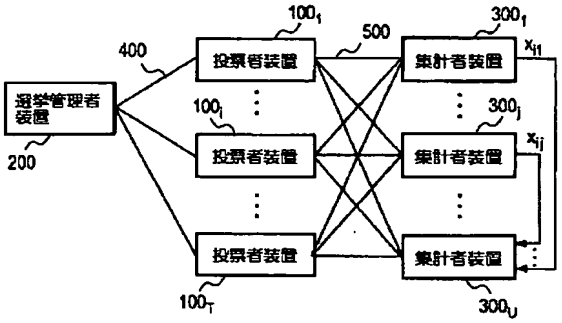


図９

【図１０】

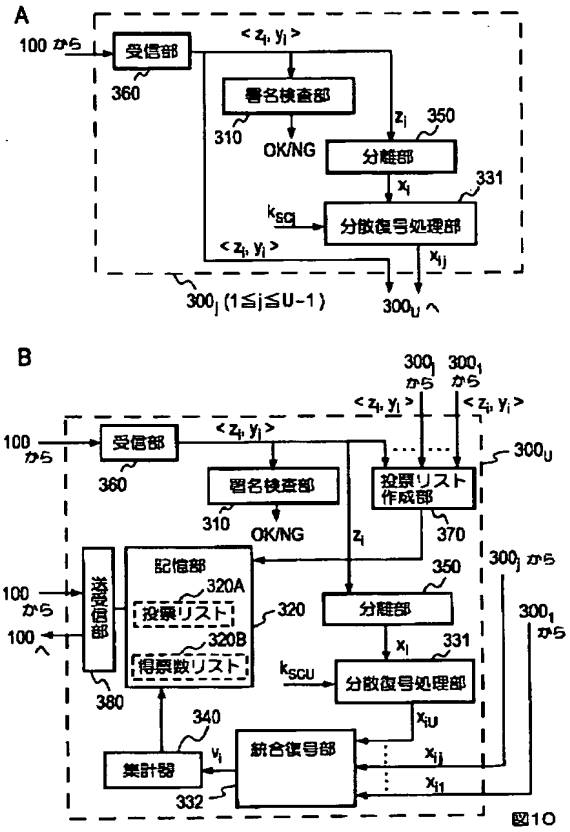


図10

【手続補正書】
【提出日】平成１１年１１月２２日（１９９９．１１．２２）
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】請求項７
【補正方法】変更
【補正内容】

【請求項７】　請求項１又は２の電子投票方法において、上記ステップ(a)は上記前処理文に対する投票者の署名を生成し、上記前処理文と共に上記管理者装置に送信するステップを含み、上記ステップ(b) は上記前処理文に対する上記投票者の署名の正当性を検査するステップを含む。